In the claims:

1. (previously amended) A method for enabling secure authentication of a user in a computerized card access transaction while performing said transaction via a computer or other device, said transaction typically associated with at least one activity performed by a user in transacting with a vendor, said vendor being a person, an entity, a computer or a machine and wherein said at least one activity is performed by the user from among a group of activities relating to acquiring of goods or services, and/or access to a computer, a network and/or virtual and physical sites, said method comprising:

providing the user with a physical card by a card issuer associated with said vendor, said card being embodied in a portable, digitally recordable medium having stored thereon a user program that does not require storage of any passwords, programs, secret keys or any component of said user program on a computer thereby preventing the possibility of such passwords or other sensitive information becoming disclosed either to an unauthorized person who may gain physical access to the user's computer or by any form of online intrusion and to enable complete portability of the method so that it is not restricted to a specific programmed computer, but is usable in conjunction with any computer equipped with a compatible operating system;

allocating to said physical card a unique identification number (ID), a password, and where applicable, an account number;

recording in a database associated with the card issuer for each card so provided, details of said ID and

said password together with details of the user to whom the card has been provided;

initiating the card transaction in one of offline and online modes, by inserting said card into the appropriate drive of the user's computer or by connecting said card to said computer in any other manner while the computer is offline;

activating said card causing it to display a login window on the computer screen;

entering the appropriate password in said login window which appears on the user's screen, so as to activate said program on said card causing a further login window to appear;

entering required information in said login window;

generating a unique one-time Cybercoupon comprising a message containing the user's ID and other relevant information,

wherein during said offline mode, said card transaction is initiated by:

communicating ~~a~~ said Cybercoupon as part of said card transaction, to the vendor in any manner not involving online communications,

and wherein during said online mode, said card transaction is initiated by:

disconnecting said card from the computer;

connecting the computer online;

communicating ~~a~~ said Cybercoupon as part of said card transaction, to the vendor via online communications;

receiving said Cybercoupon at the vendor,

processing, by the vendor of said request for authorization in accordance with its standard criteria;

authorizing the card transaction, if said Cybercoupon is determined to be valid and if standard criteria are met;

or otherwise rejecting the card transaction.

2. (previously amended) The method of claim 1 wherein when said card is activated, advertising material contained in said user program or generated by the program on said card is optionally displayed on a screen.

3. (previously amended) The method of claim 1 wherein when the computer is connected online, a vendor's order form is downloaded; and

said Cybercoupon is inserted on said order form in the position requiring a card number.

4. (previously amended) The method of claim 1 wherein said password may comprise at least a single character string and wherein said user program is designed so that if an incorrect password is entered more than a predetermined number of times, the user gains entry to said user program and a fictitious Cybercoupon is generated having the appearance of a regular Cybercoupon but containing a code which indicates to the card issuer, that an irregular attempt has been made to enter the password, thus enabling the card issuer to take such steps as it considers appropriate.

5. (previously amended) The method of claim 1, wherein said user program stored on said physical card comprises a number generator and an encryption program, which, on receiving the appropriate command, generates said one-time Cybercoupon in encrypted form, containing encrypted information relating to the card ID and, where applicable, the vendor identity and other information relating to the card transaction and wherein said processing by the vendor includes decrypting said Cybercoupon.

6. (previously amended) The method of claim 5, wherein the vendor's right to give effect to said card transaction is subject to authorization by the card issuer in accordance with a method comprising:

transmitting details of the proposed transaction by the vendor via the vendor's usual communication network to the card issuer with a request for authorization of said transaction;

receiving by a Filter Program associated with the card issuer of said request from said vendor for authorization of said transaction;

discriminating by said Filter Program between a request for authorization containing a Cybercoupon generated by the encrypted cybercoupon method and requests containing other card numbers;

forwarding by said Filter Program of a request for authorization which does not contain a Cybercoupon, to said Card Issuer's standard system for processing requests for authorization;

processing of said request and responding directly by said card issuer to said vendor;

transmitting a request which contains a Cybercoupon to a Translator Program associated with said Filter Program;

decrypting of said Cybercoupon by said Translator Program to disclose the ID and other information stipulated by the user, the identity of the vendor and whether or not said Cybercoupon contains an alert message indicating that an irregular attempt has been made to access said card;

replacing, in a message which contains said alert, said Cybercoupon with said ID and forwarding said request to the card issuer's standard system for processing said requests and marking the record in said database relating to the relevant

ID as blocked and requiring further action by said card issuer in accordance with said card issuer's policy;

checking a Cybercoupon which does not contain said alert, to ascertain whether said Cybercoupon has been used previously within a prescribed period of time, whether it originated from a valid original card issued by said card issuer to said user and that, where applicable, other information and vendor identity stipulated by said user coincide with the information in the request for authorization received from said vendor;

rejecting said request if said request fails any of said checks and notifying said vendor via said Filter Program accordingly;

substituting, in a request which has passed all said checks, the relevant ID number for said Cybercoupon and forwarding said request with said substituted ID number, to the card issuer's standard system for processing card transactions;

retaining a record of all incoming requests which contained Cybercoupons and said relevant ID numbers which have been passed to said card issuer's standard processing system;

processing of said request for authorization by said card issuer's standard processing system in accordance with said card issuer's usual criteria;

responding by said card issuer's said standard processing system to said Translator Program that said request has been rejected if said criteria have not been met or that said request has been accepted if said criteria have been met;

replacing, by said Translator Program of said ID number with said original Cybercoupon;

transmitting said response containing said Cybercoupon from said Translator Program to said vendor via said Filter Program.

7. (previously amended) The method of claim 1, wherein said card contains a quantity of Cybercodes, listed in a specific sequence, which sequence can be recycled when the last Cybercode in the list has been used, said list being associated with said card ID and said user program modified to generate a Cybercoupon by selecting one said Cybercode at a time from said list in said sequence and combining said Cybercode with said ID, said combination of ID and Cybercode constituting said Cybercoupon, said Cybercoupon being generated and processed with said Cybercode in a method comprising:

allocating to said card, in addition to said details, said quantity of Cybercodes listed in said predetermined sequence as well as a unique identification number (ID) containing an indicator which indicates that said ID is invalid unless it has been modified by one of said Cybercodes, said user program being designed to select said Cybercodes one at a time in accordance with said sequence, using said one selected Cybercode to create a Cybercoupon comprising said ID modified by the addition of said Cybercode to said ID;

maintaining at the Card issuer, a database containing, in addition to said details, said list of Cybercodes in their specified sequence;

selecting by said program when activated, while the computer is offline, of the next unused Cybercode in its predetermined sequence in said list contained on said card;

generating a Cybercoupon comprising a combination of said ID and said Cybercode and displaying it on a screen;

communicating, in an offline transaction, said ID to the vendor, in any manner not involving online communication;

connecting said computer online;

and in an online transaction, communicating said ID to the vendor online;

and in both online and offline transactions,

communicating said Cybercoupon to said card issuer, by interaction of said user program with said user's email program or browser or by any other means of communication, together with details of said transaction including where relevant, the currency, the monetary value of the transaction and the identity of the vendor;

receiving by said card issuer of said notification from said user and entering of information contained in said message received by the card issuer into said database associated with said card issuer's system and marking in said database of said Cybercode as contained in said notification as having been used and awaiting a request for authorization from said vendor;

receiving said communication by said vendor from the user;

transmitting by said vendor to said card issuer of said communication with a request for authorization of the transaction;

receiving of said request at said Card Issuer's node;

detecting from said indicator in said ID that said ID requires an authentic valid Cybercode in order to be validated;

comparing said request with the communication received from the user and with data stored in said database to ensure that within predefined deviation parameters, said Cybercode is valid and in the correct position in the predetermined sequence;

comparing that information contained in said request for authorization received from said vendor matches the information contained in said notification received from said user;

rejecting a request which fails any of said checks and notifying said vendor accordingly.

8. (previously amended) The method of claim 7, varied in that the user sends a Cybercoupon in place of said ID to the vendor and does not communicate with the card issuer and wherein authorization by the card issuer is performed in accordance with a method comprising:

transmitting details of the proposed transaction, including said Cybercoupon, by the vendor via the vendor's usual communication network to the card issuer with a request for authorization of said transaction;

receiving of said request from said vendor initially by a Filter Program at said Card Issuer's node;

differentiating by said Filter Program between requests containing Cybercoupons generated by said added Cybercode method and requests containing other card numbers;

directing by said Filter Program of a request which does not contain said Cybercoupon to the card issuer's standard processing system;

processing of said request and responding directly by said card issuer to said vendor;

forwarding a request which contains said Cybercoupon to a Translator Program associated with said Filter Program;

detecting by said Translator Program of the ID and the Cybercode contained in ~~a~~ said request;

comparing the data stored in said database to ensure that within predefined deviation parameters, said Cybercode is in the correct position in the predetermined sequence and marking that it has now been used;

rejecting a request which fails any of said checks and notifying said vendor accordingly via said Filter Program;

substituting, in a request which has passed all checks, the relevant ID in place of said Cybercoupon and transmitting said request with said substituted ID, to the card issuer's standard processing system;

retaining a record of all incoming requests which contained said indicators and said relevant ID's which have been passed to the card issuer's standard processing system;

processing of said request for authorization by the card issuer's standard processing system in accordance with its usual criteria;

responding by said card issuer's said standard processing system to said Translator Program that said request has been rejected if said criteria have not been met or that said request has been accepted if said criteria have been met;

replacing, by said Translator Program of said ID number with said original Cybercoupon in respect of a request which was originally received containing a Cybercoupon; and

transmitting said response containing said Cybercoupon by said Translator Program via said Filter Program to the vendor.

9. (previously amended) The method of claim 7, wherein said processing procedure contains a calculating means for statistically determining an acceptable tolerance in variation from said predetermined sequence of said Cybercode, taking into account such factors as the norm for the particular industry between the time and date on which a vendor receives an order and the time and date on which a Card Issuer receives the relevant request for validation from said vendor, and the value of the order, so that a transaction quoting an out of sequence Cybercode will be authorized with a statistically calculated level of safety, provided that such Cybercode falls within said calculated variation tolerance.

10. (original) The method of claim 1 wherein the card contains a store for storage of encryption keys and a commonly available encryption algorithm for encrypting a Cybercoupon for use as a password in the form of a challenge, using symmetric keys such as, but not limited to, RC4 or DES, said

challenge being used for controlling access to a computer in accordance with a method comprising:

requesting by the user of permission to logon to a server;

responding by said server with a challenge;

extracting by said user program of a key from said store;

generating a Cybercoupon by using said key in conjunction with said algorithm to encrypt said challenge;

transmitting said Cybercoupon together with the card ID to the server;

using the ID by the server to identify the key;

using said key to decrypt said Cybercoupon;

comparing the decrypted Cybercoupon with the original challenge; and

authenticating the user if said response is identical to said challenge.

11. (original) The method of claim 10 using asymmetric keys.

12. (original) The method of claim 1 wherein the card contains a store for storage of encryption keys and a commonly available encryption algorithm for encrypting text which encrypted text can be stored securely on a local or remote computer or transmitted as a message electronically.

13. (original) The method of claim 12 wherein said user program interacts with the user's email program to generate secure encrypted messages by email.

14. (original) The method of claim 1, wherein said card takes the form of a combined magnetic stripe card and a smartcard in one unit, enabling said user to choose to use said card either as a conventional magnetic card or as a smartcard, said combined card containing a conventional magnetic stripe and

any one of said user program described herein for generating Cybercoupons or passwords.

15. (previously amended) The method of claim 1 wherein said card contains a Dual Tone Multifrequency (DTMF) Generator in addition to said user program which interacts therewith in accordance with a conversion method so as to convert said Cybercoupon to an audio tone Cybercoupon, each digit in said Cybercoupon being converted to a specific audio frequency in accordance with international telephony standards.

16. (previously amended) The method of claim 1 wherein said card contains a store for storage of encryption keys and a commonly available encryption algorithm for encrypting a Cybercoupon for use as a password in the form of a challenge, using symmetric keys or asymmetric keys and wherein said card contains a Dual Tone Multifrequency (DTMF) Generator in addition to said user program which interacts therewith in accordance with a conversion method so as to convert said Cybercoupon to an audio tone Cybercoupon, each digit in said Cybercoupon being converted to a specific audio frequency in accordance with international telephony standards, said challenge being used for controlling access to a remote computer in a method comprising:

generating a request for permission to logon to a server;

converting said request to an audio signal recognizable by said server;

transmitting said audio signal to the server;

responding by said server with an audio challenge;

converting said audio challenge to text;

extracting by said user program of an encryption key from said store;

using said encryption key to generate a Cybercoupon comprising said challenge encrypted using said algorithm;

converting said Cybercoupon to an audio tone Cybercoupon and converting said ID to an audio signal;
transmitting said audio tone Cybercoupon in response together with the audio card ID to the server;
using the ID by the server to identify said encryption key;
using said encryption key to decrypt said Cybercoupon;
comparing the decrypted response with the original challenge;
authenticating the user if said response is identical to said challenge.

17. (original) The method of claim 15 wherein said DTMF card is self-contained and operates without the use of a separate computer, said DTMF card including a keypad, a speaker and optionally a screen in addition to said user program and said DTMF generator, thus enabling a Cybercoupon to be generated, converted into audio tones and transmitted by placing the speaker on the card close to the microphone of the telephone or other means of audio communication.

18. (previously amended) The method of claim 15 wherein said DTMF-card is used in association with a telephone calling card provided by a telephony service provider, said Cybercoupon comprising the user's ID and PIN encrypted and converted to audio signals as described.

19. (previously amended) The method as recited in claim 1, whereby a POS Module is provided at an outlet equipped with commercial Point of Sale (POS) software, said module being designed to interact with said outlet's POS software enabling said POS Module to activate said card, read said Cybercoupon generated by said card and treat said Cybercoupon as a regular card number for processing in the usual manner adopted by said

outlet.

20. (currently amended) A method for ~~preventing fraudulent card transactions in systems such as card payment and card access systems, while performing a card transaction,~~ enabling secure authentication of a user in a card access transaction, said transaction typically associated with at least one activity performed by a user in transacting with a vendor, and wherein said at least one activity is performed by the user from among a group of activities relating to acquiring of goods or services, and/or access to a computer, a network and/or virtual and physical sites, said method comprising:

providing the user with a physical card by a card issuer, said card being embodied in a non-digital portable medium such as paper or plastic,

allocating to said physical card at least a unique card number and optionally an account number as well as a quantity of Cybercodes listed in a predetermined sequence and in which an indicator in said card number indicates that said card number is invalid unless it has been modified by said Cybercode and wherein, the user selects one Cybercode at a time in accordance with said sequence and uses said Cybercode to create a Cybercoupon comprising said card number modified by the addition of said Cybercode as an extension to said card number or by inserting said Cybercode in said card number in replacement of the equivalent number of digits in a predetermined position in said card number, said Cybercoupon being used in lieu of the user's card number when initiating a card transaction;

recording in a database associated with the card issuer for each card so provided, details of said card number and where applicable said account number together

with said list of Cybercodes in said sequence and details of the user to whom the card has been provided;

providing the user with said list of Cybercodes in a document separate from the card itself;

preparing, by the user when a transaction is to be effected, of said Cybercoupon by combining said card number with the next available Cybercode in its predetermined sequence;

initiating the card transaction by communicating said Cybercoupon as part of said transaction, to the vendor in any manner whether or not involving online communications,

receiving said Cybercoupon at the vendor;

transmitting by the vendor to the card issuer of a request for authorization of the card transaction,

receiving said request for authorization at the card issuer; and

processing the card transaction, in accordance with an authorization method comprising:

receiving of said request initially by a Filter Program at the card issuer;

differentiating by said Filter Program between requests containing Cybercoupons generated by said added Cybercode method and requests containing other card numbers;

directing by said Filter Program of a request which does not contain said Cybercoupon to the card issuer's standard processing system and responding accordingly directly by the card issuer to the vendor;

forwarding a request which contains said Cybercoupon to a Translator Program associated with said Filter Program;

detecting by said Translator Program of the card number and the Cybercode used in a request containing a Cybercoupon;

comparing the data stored in said database to ensure that within predefined deviation parameters said Cybercode is in the correct position in the predetermined sequence and marking that it has now been used;

rejecting a request which fails any of said checks and notifying said vendor accordingly via said Filter Program;

substituting, in a request which has passed all checks, the relevant card number for said Cybercoupon and transmitting said request with said substituted card number, to the card issuer's standard processing system;

retaining a record of all incoming requests which contained Cybercoupons and said relevant card numbers which have been passed to the card issuer's standard processing system;

processing of said request for authorization by the card issuer's standard processing system in accordance with its standard criteria;

responding by said card issuer's ~~said~~ standard processing system to said Translator Program that said request has been rejected if said criteria have not been met;

responding by said card issuer's ~~said~~ standard processing system to said Translator Program that said request has been accepted if said criteria have been met;

replacing, by said Translator Program of said card number with said original Cybercoupon;

transmitting said response containing said Cybercoupon by said Translator Program to said Filter Program;

transmitting said response by the Filter Program to the vendor; and

transmitting said response to the user.

21. (previously amended) The method of claim 20 wherein the user is supplied, in a document separate both from said card and from said list of Cybercodes, with a unique supplementary code to be used in conjunction with said card number so that an unauthorized person who obtains access to said list of Cybercodes is unable to use said Cybercodes without knowledge of said supplementary code.

22. (previously amended) A system for enabling secure authentication of a user in a computerized card access transaction while performing said transaction via a computer or other device, said transaction typically associated with at least one activity performed by a user in transacting with a vendor, said vendor being a person, an entity, a computer or a machine and wherein said at least one activity is performed by the user from among a group of activities relating to acquiring of goods or services, and/or access to a computer, a network and/or virtual and physical sites, said system comprising:

a physical card provided by a card issuer, said card being embodied in a portable, digitally recordable medium having stored thereon a user program that does not require storage of any passwords, programs, secret keys or any component of said user program on a computer thereby preventing the possibility of such passwords or other sensitive information becoming disclosed either to an unauthorized person who may gain physical access to

the user's computer or by any form of online intrusion and to enable complete portability of the method so that it is not restricted to a specific programmed computer, but is usable in conjunction with any computer equipped with a compatible operating system, said physical card having allocated thereto at least a unique identification number (ID) and a password, and where applicable, an account number; and

a database associated with the card issuer for each card having recorded therein, details of said ID, said password and where applicable, said account number, together with details of the user to whom the card has been provided;

wherein said card is used to perform a card transaction initiated by:

inserting said card into the appropriate drive of the user's computer or otherwise connecting said card to said computer while the computer is offline;

activating the said card causing it to display a login window on the computer screen;

entering the appropriate password in said login window which appears on the user's screen, so as to activate said program on said card causing a further login window to appear;

entering required information in said login window;

generating a unique one-time Cybercoupon comprising an encrypted message containing the user's ID and other relevant information,

and wherein during said offline mode, said card transaction is initiated by:

communicating said Cybercoupon as part of said transaction, to the vendor in any manner not involving online communications,

and wherein during said online mode, said card transaction is initiated by:

disconnecting, automatically, said card from the computer;

connecting the computer online;

communicating said Cybercoupon as part of said card transaction, to the vendor via online communications;

receiving said Cybercoupon at the vendor, and processing said card transaction by the vendor;

transmitting by the vendor to the card issuer via a communication network, a request for authorization of the card transaction, if the vendor requires authorization by the card issuer before said vendor is entitled to give effect to said transaction;

receiving said request for authorization at the card issuer;

processing, by the card issuer of said request for authorization in accordance with its standard criteria;

authorizing the card transaction, if said Cybercoupon is determined to be valid and if the card issuer's standard criteria are met;

or otherwise rejecting the card transaction.